



<b>TRANSMITTAL OF APPEAL BRIEF</b>			Docket No. SONY 3.0-029
In re Application of: Paul H. Feinberg			
Application No. 09/837,283	Filing Date April 18, 2001	Examiner T. B. Truong	Group Art Unit 2135
Invention: DEVICE AUTHENTICATION			

**TO THE COMMISSIONER FOR PATENTS:**

Transmitted herewith is the Appeal Brief in this application.

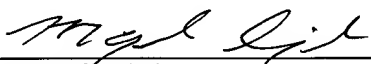
The fee for filing this Appeal Brief is 500.00.

☒ Large Entity ☐ Small Entity

☐ A check in the amount of \_\_\_\_\_ is enclosed.

☒ Charge the amount of the fee to Deposit Account No. 12-1095.  
This sheet is submitted in duplicate.

☒ The Commissioner is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 12-1095.  
This sheet is submitted in duplicate.

  
\_\_\_\_\_  
Mayush Singhvi  
Attorney Reg. No. : 50,431  
LERNER, DAVID, LITTENBERG, KRUMHOLZ &  
MENTLIK, LLP  
600 South Avenue West  
Westfield, New Jersey 07090  
(908) 654-5000

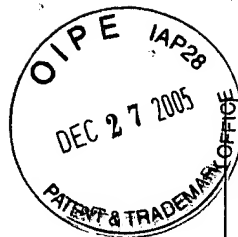
Dated: December 22, 2005

LD-546\

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the U.S. Postal Service on the date shown below with sufficient postage as First Class Mail, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Dated: December 22, 2005

Signature:  (Mayush Singhvi)



I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: December 22, 2005 Signature: *Mayush Singhvi*

(Mayush Singhvi)

Docket No.: SONY 3.0-029  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:  
Paul H. Feinberg

Application No.: 09/837,283

Group Art Unit: 2135

Filed: April 18, 2001

Examiner: T. B. Truong

For : DEVICE AUTHENTICATION

**APPEAL BRIEF**

MS Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

This is an appeal from the final rejection of claims 1-33 mailed May 19, 2005. An extension of time in which to file the Brief, believed originally to be due October 22, 2005, is hereby requested. The Commissioner is hereby authorized to charge the extension of time fee along with the \$500.00 required by 37 C.F.R. § 41.20(b)(2) for filing the brief, and any other fees that may be due and owing in connection with the brief, to Deposit Account No. 12-1095.

**REAL PARTIES IN INTEREST**

12/29/2005 HDESTA1 00000015 121095 09837283  
01 FC:1402 500.00 DA

The real parties in interest in this case are the assignees of record: Sony Corporation, a Japanese corporation, having a place of business at 7-35 Kitashinagawa 6 Chome, Shinagawa-ku, Tokyo, Japan; and Sony Electronics Inc., a New Jersey corporation, having a place of business at 1 Sony Drive, Park Ridge, New Jersey 07656. The assignment of the present

application to Sony Corporation and Sony Electronics Inc. was recorded in the United States Patent and Trademark Office on August 9, 2001 and at Reel 012067, Frame 0047.

**RELATED APPEALS AND INTERFERENCES**

At present, there are no other appeals or interferences known to Appellant, the Appellant's legal representative or the assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

**STATUS OF CLAIMS**

Claims 1-33 are pending in the present application. Claims 1-33 were rejected in a final office action and such final rejection of claims 1-33 is being appealed.

**STATUS OF AMENDMENTS**

A Final Office Action rejecting claims 1-33 was mailed on May 19, 2005. No amendment has been filed subsequent to the mailing of the Final Office Action.

**SUMMARY OF CLAIMED SUBJECT MATTER**

Before discussing the Examiner's final rejection and the references applied therein, Appellant provides the following summary.

Independent claim 1 is directed to a method of transferring information between devices upon a connection and

reconnection thereof. Here, a first device (or module) is provided which has a first identifier and a second device (or toy) is provided which has a second identifier. (Spec pg. 5, lines 19-21 and pg. 6, lines 1-2.) When the module and toy are first connected, the module sends the first identifier to the toy and the toy sends the second identifier to the module. (Spec pg. 11, lines 8-9.) The first identifier is stored in the toy and the second identifier is stored in the module. After the module and toy are disconnected and subsequently reconnected, both the module and the toy transmit their respective identifiers to each other. *The module and toy then compare the respective received identifiers to the previously stored identifiers.* (Italics added for emphasis.) Depending upon the results of such comparison (for example, if the received identifiers match the previously stored identifiers) additional information may be transmitted from the module to the toy and/or from the toy to the module. (Spec pg. 11, line 12 to pg. 14, line 2.)

Claim 8 is directed to a method for authenticating a device. Here, a first value may be received from the device, in which the first value is different from an identifier associated with the device. (Spec pg. 6, line 9 to pg. 8, line 10.) The identifier is determined from the value, in which the value is a function of the identifier *and the number of times the device has been authenticated.* (Italics added for emphasis.) The identifier determined from the value may be compared against a pre-stored identifier. (Spec pg. 6, line 9 to pg. 8, line 10 and pg. 9, lines 1-11.) The device may be authenticated based on the result of the comparison. (Spec pg. 12, lines 10-14.)

As one of ordinary skill can appreciate, there is an added level of security in the method of claim 8. That is, in addition to using the identifier, the method of claim 8 also

uses the number of time the device has been authenticated in determining the value.

Claims 17 is directed to a system which takes an action in response to a signal from a device. Here, the system has an *increment counter associated with a value representing the number of times the system has taken an action in response to a signal from the device.* (Italics added for emphasis.) The system also has a pseudo-random number generator which uses the increment counter value as a seed, (spec pg. 6, line 9 to pg. 8, line 10) and a memory which stores a value identifying the device. (Spec pg. 5, lines 19-21 and pg. 6, lines 1-2.) The system may have instructions including using the value of the increment counter to extract the value identifying the device from a value transmitted from the device, comparing the identification value with the value stored in memory, and taking an action dependant upon the results of the comparison. (Spec pg. 6, line 9 to pg. 8, line 10; pg. 9, lines 1-11; and pg. 12, lines 10-14.)

Claim 23 is directed to a method of a destination being authenticated by a source comprising the destination. Here, a seed value is maintained which is equivalent to a seed value maintained at the source, in which the seed changes over time. A value based on the seed and based on a value identifying the destination is generated which is different from the seed and the destination's identification value. (Spec pg. 6, line 9 to pg. 8, line 10.) The generated value is transmitted to the source and authenticated so that information may be received from the source or information may be sent which will be used by the source. The authentication may be dependant upon the source using the seed to extract the destination's identification value and comparing the destination's identification value with the value of a destination known by the source to be authentic.

(Spec pg. 6, line 9 to pg. 8, line 10; pg. 9, lines 1-11; and pg. 12, lines 10-14.)

Claim 32 is directed to a system comprising a first device having an identifier and a pseudo-random number generator, and a second device. In the system, the first device sends a value to the second device based on an output from the pseudo-random number generator and the identifier. As an example, the pseudo-random number generator may generate such output by taking an index value that represents the number of times the first device and second device have communicated with each other and calculating a pseudo-random number therefrom. (Spec pg. 6, line 9 to pg. 8, line 10) *The second device receives the value and compares it to a prestored value.* (Italics added for emphasis.) (Spec pg. 9, lines 1-11.) Depending upon the results of the comparison (for example, if the received value matches the prestored value), the two devices may communicate further. (Spec pg. 12, lines 10-14)

**GROUND'S OF REJECTION TO BE REVIEWED ON APPEAL**

1. Whether claims 8-16 and 23-31 are anticipated under 35 U.S.C. §102(b) by U.S. Patent No. 5,109,152 issued to Takagi et al. ("Takagi")?
2. Whether claims 8 and 23 are anticipated under 35 U.S.C. §102(b) by U.S. Patent No. 5,355,413 issued to Ohno ("Ohno")?
3. Whether claims 1-7 are unpatentable under 35 U.S.C. §103(a) based on Takagi?
4. Whether claims 17-22 and 32-33 are unpatentable under 35 U.S.C. §103(a) based on Takagi in view of U.S.

Patent No. 5,651,123 issued to Nakagawa et al.  
("Nakagawa")?

**GROUPING OF CLAIMS**

For the purpose of the present appeal, the Appellant requests that the claims be grouped as follows:

- I. Claims 8 and 23 stand or fall together.
- II. Claims 9-16 and 24-31 stand or fall together.
- III. Claims 1-7 stand or fall together.
- IV. Claims 17-22 stand or fall together.
- V. Claims 32-33 stand or fall together.

**ARGUMENT**

**I. Rejection under 35 U.S.C. §102(b) by Takagi.**

Claims 8-16 and 23-31 are not anticipated by U.S. Patent No. 5,109,152 issued to Takagi for at least the reasons described below.

Independent claim 8 recites in part as follows:

"... receiving a first value from the device,  
the first value being different from an  
identifier associated with the device;

determining the identifier from the value,  
the value being a function of the identifier  
and the number of times the device has been  
authenticated..."

Accordingly, in the method of claim 8, the identifier is determined from a value which is a function of the identifier and the number of times the device has been authenticated. Thus, the number of times a device has been authenticated (or index value) is utilized in determining the identifier which, in turn, is used in the authenticating of the device. For example, as described on pages 6 to 8 of the present application, if the index value (number of times the device has been authenticated) is 1, then the pseudorandom number generator may obtain the first prime number after four (which is 5), divide it by the next prime number (which is 7), and then take the first and second numbers after the decimal point which is 71. The pseudo random number 71 may be added to the module (or device) ID (25) to obtain a value of 96. As another example, if the index value was 3, then the pseudorandom number generator may obtain the third prime number after four (which is 11), divide it by the next prime number (which is 13), and then take the third and fourth numbers after the decimal point which is 61, which would result in a value of 86.

In section 8 of the Final Office Action mailed May 19, 2005, the Examiner asserted that Takagi discloses that first comparison means 116 compares random number data  $R_2$  produced by IC card 110 with random number data  $R_0$  provided by a first random number generation means 111. If  $R_2$  and  $R_0$  match, information may be exchanged between first processing means 120 and transaction IC card 150. Further, and as best understood, it appears that the Examiner asserted that Takagi also utilizes the number of times the IC card has been authorized or authenticated in determining whether such information could be exchanged. (See lines 18-21 of page 14 of the May 19<sup>th</sup> Final Office Action.)

Contrary to the Examiner's apparent assertion, Takagi does not disclose using the "number of times the device has been



authenticated" for a value used to determine the identifier. Accordingly, Takagi does not anticipate independent claim 8 as well as dependent claims 9-16 which depend therefrom.

Independent claim 23 recites in part as follows:

"maintaining a seed value which is equivalent to a seed value maintained at the source, the seed changing over time, generating a value based on the seed and based on a value identifying the destination whereby the generated value is different from the seed and the destination's identification value; . . . the authentication being dependant upon the source using the seed to extract the destination's identification value and comparing the destination's identification value with the value of a destination known by the source to be authentic."

Accordingly, the method of claim 23 specifically recites a "seed value" or "seed." As described throughout the present specification, such seed value may correspond to the number of times a device (such as the destination or source) has been authenticated. Takagi does not disclose utilizing the number of times a device has been authenticated (or "seed value") in his authenticating method. Thus, Takagi does not disclose maintaining a seed value which is equivalent to a seed value maintained at the source, the seed changing over time, generating a value based on the seed and based on a value identifying the destination whereby the generated value is different from the seed and the destination's identification value, and authenticating the destination using the seed to

extract the destination's identification value, as in claim 23. Therefore, claim 23, as well as claims 24-31 which depend therefrom are not anticipated by Takagi.

## II. Rejection under 35 U.S.C. §102(a) by Ohno.

Claims 8 and 23 are not anticipated by U.S. Patent No. 5,355,413 issued to Ohno for at least the following reasons.

Ohno is directed to an authentication method using the encryption of an authentication code and a time data item. More specifically, in Ohno, an IC card and a terminal have multiple authentication codes stored in a memory, each code having a corresponding time data item. One of the authentication codes is selected and encrypted before being sent to the other device. In addition, the time data item associated with the selected authentication code is also sent to the other device. In the other device, the authentication code corresponding to the received time data is obtained and encrypted before comparing it to the received encrypted authentication code. (Ohno, Abstract.)

Accordingly, Ohno appears to merely select a stored authentication code and encrypt the same. As such, Ohno does not use "the number of times the device has been authenticated" in generating the encrypted authentication code that is sent to the other device. Thus, since Ohno does not disclose "determining the identifier from the value, the value being a function of the identifier and the number of times the device has been authenticated" as in claim 8, Ohno does not anticipate claim 8.

Additionally, Ohno does not disclose utilizing the number of times a device has been authenticated (or "seed value") in his authenticating method. Thus, Ohno does not disclose maintaining a seed value which is equivalent to a seed

value maintained at the source, the seed changing over time, generating a value based on the seed and based on a value identifying the destination whereby the generated value is different from the seed and the destination's identification value, and authenticating the destination using the seed to extract the destination's identification value, as in claim 23.

### III. Rejection under 35 U.S.C. §103(a) by Takagi.

Claims 1-7 are patentable over U.S. Patent No. 5,109,152 issued to Takagi for at least the following reasons.

Claim 1 recites in part as follows:

"the first device storing the second identifier and the second device storing the first identifier;

when the first and second devices are disconnected and reconnected, the first device sending the first identifier to the second device and the second device sending the second identifier to the first device during the first reconnection, and each device comparing the received identifier against the stored identifier and sending additional information to the other device depending upon the result of the comparison"

Accordingly, in the method of claim 1, the second identifier which was previously stored in the first device and the first identifier which was previously stored in the second device are respectively compared to the first and second identifiers which are sent by the appropriate device to the other device during a reconnection. Takagi does not teach or suggest such feature of claim 1. Takagi does not disclose storing information (such as identifiers) that is utilized when the devices are reconnected at a subsequent time. Instead, Takagi authenticates an IC card every time the card is entered

into a card reader. Accordingly, claim 1, as well as claims 2-7 which depend therefrom, are patentable over Takagi.

**IV. Rejection under 35 U.S.C. §103(a) by Takagi over Nakagawa.**

Claims 17-22 and 32-33 are patentable over U.S. Patent No. 5,109,152 issued to Takagi et al. in view of U.S. Patent No. 5,651,123 issued to Nakagawa et al. for at least the following reasons.

Independent claim 17 recites in part as follows:

"...an increment counter associated with a value representing the number of times the system has taken an action in response to a signal from the device;

a pseudo-random number generator using the increment counter value as a seed;"

In the Final Office Action, the Examiner admitted that Takagi does not disclose an increment counter as in claim 17. In an attempt to cure this defect, the Examiner relies on the incrementor 302 of Nakagawa.

It is respectfully submitted that the incrementor 302 of Nakagawa is substantially different from the increment counter of claim 17. That is, unlike the increment counter of claim 17, the incrementor 302 of Nakagawa is not associated with a value representing the number of times the system has taken an action in response to a signal from the device. (An example of such action may be the number of times a device has been authenticated.) Instead, Nakagawa merely discloses that the incrementor 302 increments the contents of a program counter. The output of the program counter is used to output an address

for reading an instruction word from the instruction memory.  
(Nakagawa, col. 1, lines 48-55.)

Thus, it is respectfully submitted that claim 17 is distinguishable over the applied combination of Takagi and Nakagawa.

Claim 32 is patentable over the applied combination of Takagi and Nakagawa. In claim 32, a first device sends a value "based on the output of a pseudo-random number generator and an identifier." The second device receives the value, "compares the received value with a prestored value," and sends or receives information depending upon the outcome of the comparison. Neither Takagi nor Nakagawa as applied by the Examiner discloses the above features of claim 32.

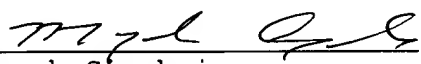
Additionally, there is no motivation or suggestion to combine Takagi and Nakagawa. That is, Takagi is directed to an authentication method, while Nakagawa is directed to a device for executing stored instructions. One skilled in the art seeking to construct an authentication device or method would not seek to utilize a program execution device which stores program instructions in an address sequentially designated with a pseudo-random number sequence.

**CONCLUSION**

For all of the reasons set forth in Appellant's Appeal Brief, the final rejection of claims 1-33 should be reversed.

Dated: December 22, 2005

Respectfully submitted,

By   
Mayush Singhvi  
Registration No.: 50,431  
LERNER, DAVID, LITTENBERG,  
KRUMHOLZ & MENTLIK, LLP  
600 South Avenue West  
Westfield, New Jersey 07090  
(908) 654-5000  
Attorney for Applicant

**APPENDIX A - CLAIMS**

1. (original) A method of transferring information between devices upon connection and reconnection comprising:

providing a first device having a first identifier;

providing a second device having a second identifier;

the first device sending the first identifier to the second device during a first connection;

the second device sending the second identifier to the first device during the first connection;

the first device storing the second identifier and the second device storing the first identifier;

when the first and second devices are disconnected and reconnected, the first device sending the first identifier to the second device and the second device sending the second identifier to the first device during the first reconnection, and each device comparing the received identifier against the stored identifier and sending additional information to the other device depending upon the result of the comparison.

2. (original) The method of claim 1 wherein the step of sending an identifier to the other device includes sending a value that is based on, but not equivalent to, the identifier.

3. (original) The method of claim 2 wherein the value sent by the first device is based on the number of times the first device has connected to the second device.

4. (original) The method of claim 3 wherein the difference between the different values sent each time is pseudo-random.

5. (original) The method of claim 3 wherein the value sent by the first device is determined based on at least one mathematical operation, and at least one of the purposes of

the mathematical operation is to make it difficult to predict the next value to be sent.

6. (previously presented) The method of claim 2 wherein the value sent by the first device is based on one or more mathematical operations using at least the identifier, the number of times the first device has connected to the second device, and a third number as operands.

7. (original) The method of claim 6 wherein the third number is a prime number.

8. (original) A method of authenticating a device comprising:

receiving a first value from the device, the first value being different from an identifier associated with the device;

determining the identifier from the value, the value being a function of the identifier and the number of times the device has been authenticated;

comparing the identifier determined from the value against a pre-stored identifier;

authenticating the device based on the result of the comparison.

9. (original) The method of claim 8 further including: receiving a second value from the device after the step of authenticating, this value being different from the first value and different from the identifier; determining the identifier from the second value, the second value being a function of the identifier and the number of times the device has been authenticated; comparing the identifier determined from the second value against a pre-stored identifier; authenticating the device again based on the result of the comparison.

10. (original) The method of claim 9 wherein the pre-stored value is stored by: receiving an initial value from the device, the initial value being different from the



identifier, the first value and the second value; determining the identifier from the initial value, the initial value being a function of the identifier; storing the initial value.

11. (original) The method of claim 10 wherein the difference between the initial value and the second value is different from the difference between first value and the second value.

12. (original) The method of claim 8 further including sending information to the device dependant upon whether the device is authenticated.

13. (original) The method of claim 8 further using information from the device dependant upon whether the device is authenticated.

14. (original) The method of claim 13 further including taking an action dependent upon whether the device is authenticated.

15. (original) The method of claim 8 wherein the function is a pseudo-random generator using the number of times the device have been authenticated as a seed.

16. (original) The method of claim 8 wherein the function is intended to make it difficult to predict the next value to be received.

17. (original) A system which takes an action in response to a signal from a device, the system comprising: an increment counter associated with a value representing the number of times the system has taken an action in response to a signal from the device; a pseudo-random number generator using the increment counter value as a seed; memory for storing a value identifying the device; instructions including using the value of the increment counter to extract the value identifying the device from a value transmitted from the device, comparing the identification value with the value stored in memory, and taking the action dependant upon the results of the comparison.

18. (original) The system of claim 17 wherein the device includes: an increment counter; a random number generator using the increment counter of the device value as a seed; and instructions for using the value of the increment counter of the device to create a value for transmission.

19. (original) The system of claim 18 wherein the system is a toy and the device defines functions to be performed by the toy.

20. (original) The system of claim 19 wherein the toy is a doll.

21. (original) The system of claim 17 wherein if the increment counter indicates that the system has not yet taken an action in response to a signal from the device, then the system stores the identification value in memory.

22. (original) The system of claim 21 wherein the system is a lock and the action taken is locking or unlocking.

23. (original) A method of a destination being authenticated by a source comprising the destination: maintaining a seed value which is equivalent to a seed value maintained at the source, the seed changing over time, generating a value based on the seed and based on a value identifying the destination whereby the generated value is different from the seed and the destination's identification value; transmitting the generated value to the source; and being authenticated to receive information from the source or send information which will be used by the source, the authentication being dependant upon the source using the seed to extract the destination's identification value and comparing the destination's identification value with the value of a destination known by the source to be authentic.

24. (original) The method of claim 23 wherein the seed is based on the number of times the destination has sent the generated value.

25. (original) The method of claim 24 wherein the seed is based on the number of times the destination has been authenticated.

26. (original) The method of claim 25 wherein the generated number is also based on the last generated value sent from the destination to the source.

27. (original) The method of claim 23 further comprising the source: generating a value different from the seed but based on the seed; transmitting the generated value to the destination.

28. (original) The method of claim 27 wherein the value generated by the destination is also based on the last generated value transmitted from the source to the destination.

29. (original) The method of claim 28 wherein the value generated by the source is also based on the last generated value transmitted from the destination to the source.

30. (original) The method of claim 23 further comprising the source: generating a value based on the seed and based on a value identifying the source whereby the generated value is different from the seed and the source's identification value; transmitting the generated value to the source; and being authenticated to receive information from the destination or send information which will be used by the destination, the authentication being dependant upon the destination using the seed to extract the source's identification value and comparing the source's identification value with the value of a source known by the destination to be authentic.

31. (original) The method of claim 30 wherein the destination is not authenticated if the destination has already been authenticated a predetermined number of times.

32. (original) A system of devices comprising:  
a first device having an identifier and pseudo-random number generator;

a second device;

and whereby upon the connection of the first device to the second device, the first device sends a value based on the output of the pseudo-random number generator and identifier, the second device receives the value, compares the received value with a prestored value, and depending on the results of the comparison, sends or receives information to or from the first device.

33. (original) The system of claim 32 wherein the second device further comprises a checksum algorithm providing a value indicative of whether the prestored value was erased.

**APPENDIX B - EVIDENCE**

None.

Application No.: 09/837,283

Docket No.: SONY 3.0-029

**APPENDIX C - RELATED PROCEEDINGS**

None.